

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-108819

(43)Date of publication of application : 12.04.2002

(51)Int.Cl.

G06F 15/00

H04L 9/08

H04L 9/32

(21)Application number : 2000-299427

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 29.09.2000

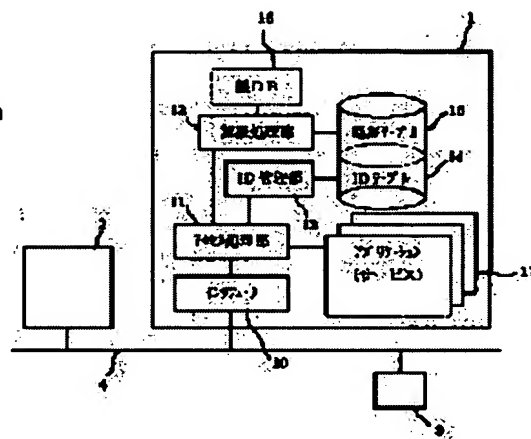
(72)Inventor : KAMIYAMA YOHEI
IMAI AKIRA

(54) INNER-COMPANY COMMUNICATION SYSTEM AND AUTHENTICATION SERVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an inner-company communication system and an authentication server for accessing an application repeatedly by a single authentication procedure.

SOLUTION: An ID control part 12 judges whether an ID number and a password transmitted from a user terminal 3 is registered in an ID table 14. When it is registered, an authentication processing part 15 selects an unallocated key from a key DB 16 and transmits it to the terminal 3. When a key is allocated, the terminal 3 embeds the allocated key to a packet for the request of access in the case of accessing an application 17.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-108819
(P2002-108819A)

(43) 公開日 平成14年4月12日 (2002.4.12)

(51) Int.Cl. ⁷	識別記号	F I	キーワード (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5 B 0 8 5
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 J 1 0 4
9/32			6 7 3 A

審査請求 未請求 請求項の数 4 O L (全 6 頁)

(21) 出願番号 特願2000-299427 (P2000-299427)

(22) 出願日 平成12年9月29日 (2000.9.29)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 神山 洋平

東京都府中市東芝町1番地 株式会社東芝
府中事業所内

(72) 発明者 今井 彰

東京都府中市東芝町1番地 株式会社東芝
府中事業所内

(74) 代理人 100083161

弁理士 外川 英明

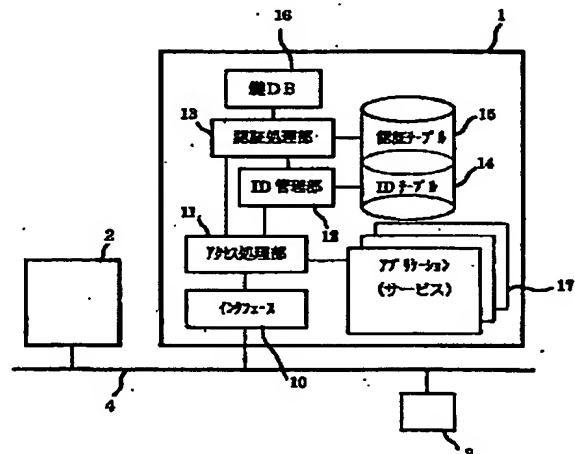
最終頁に続く

(54) 【発明の名称】 企業内通信システムおよび認証サーバ

(57) 【要約】

【課題】 一度の認証手続で、繰返しアプリケーションにアクセスすることを可能にする企業内通信システムおよび認証サーバを提供する。

【解決手段】 ID管理部12がユーザ端末3から送信されたID番号とパスワードがIDテーブル14に登録されているか判定し、登録されている場合、認証処理部15は鍵DB16から未割当ての鍵を選択してユーザ端末3へ送信する。鍵の割当てがあるとユーザ端末3は、アプリケーション17にアクセスする際には、アクセス要求にかかるパケットに割当てられた鍵を埋め込んで行う。



【特許請求の範囲】

【請求項1】 サーバコンピュータと複数のユーザ端末からなり、前記サーバコンピュータが様々なサービスを提供する企業内通信システムにおいて、

前記サーバコンピュータは、

前記サービスへのアクセス権限を標章する複数の鍵を保持する鍵データベースと、ユーザ毎に登録される識別情報とパスワードとを含むユーザ情報データベースと、ユーザに対して割当てられた鍵とユーザ名とを対にして保持する認証テーブルと、前記ユーザ情報データベースを参照してユーザの正当性を判定するユーザ情報管理部と、該ユーザ情報管理部で正当なユーザであると判定されたときにユーザ端末に対して前記鍵を割当てる認証処理部とを有し、

前記ユーザ端末は、

前記サーバコンピュータによって割当てられた鍵を受信し、前記サーバコンピュータの提供するサービスにアクセスする際に、アクセス要求に前記割当てられた鍵を含めることを特徴とする企業内通信システム。

【請求項2】 前記鍵は、文字または数字、若しくは文字と数字との組み合わせからなることを特徴とする請求項1記載の企業内通信システムシステム。

【請求項3】 前記サーバコンピュータによって前記ユーザ端末に割当てられた鍵は、一定時間が経過すると無効になることを特徴とする請求項1記載の企業内通信システムシステム。

【請求項4】 サービスを提供するサーバコンピュータへアクセスするため、ユーザ端末からの認証要求に基づき認証処理を実行する認証サーバにおいて、

前記サービスへのアクセス権限を標章する複数の鍵を保持する鍵データベースと、

ユーザ毎に登録される識別情報とパスワードとを含むユーザ情報データベースと、

ユーザに対して割当てられた鍵とユーザ名とを対にして保持する認証テーブルと、

前記ユーザ情報データベースを参照してユーザの正当性を判定するユーザ情報管理部と、該ユーザ情報管理部で正当なユーザであると判定されたときにユーザ端末に対して前記鍵を割当てる認証処理部とを具備したことを特徴とする認証サーバ。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、複数のユーザによりアクセスされるサーバコンピュータに係り、特に、アクセスしようとするユーザがアクセス権を有しているか判断する企業内通信システムおよび認証サーバに関する。

【0002】

【従来の技術】 企業内には、インターネットで用いられているTCP/IPやブラウザを利用したイントラネッ

トと呼ばれる企業内通信システムが構築されていることがあるが、この企業内通信システムに接続されているサーバコンピュータは、企業内のユーザに対して、掲示板、経理システム、勤務システム等のサービスを提供している。このようなイントラネットのサーバコンピュータが提供するサービスのうちいくつかのものについては、セキュリティ上の問題から管理職等の一定の役職についている者のみがアクセス可能等、一定の範囲内の者にアクセス権限を限定した方が望ましい場合がある。また、ユーザ全員がアクセス可能なサービスであっても、やはり外部からの不要なアクセスを排除する必要がある。このため、セキュリティ管理の必要なサービスに対するアクセスを行う場合には、ユーザ毎に割り当てた識別番号（ID番号）とユーザ各自が設定するパスワードをログイン時に入力させ、登録されているID番号とパスワードと一致した場合にのみ、アクセスを許可するといった認証方法が採用されている。

【0003】

【発明が解決しようとする課題】 しかしながら、上述の認証方法にもまだ解決すべき課題が残されている。すなわち、イントラネット上では通常複数のサーバコンピュータが存在し、さらに様々なサービス（アプリケーション）が存在しているが、各ユーザは個々のサービスにアクセスする度にID番号とパスワードを入力する必要があり、サービスにアクセスするために煩雑な手続を何度も繰返さなければならなかった。そこで、本発明は上記課題を解決し、複数あるサービスにアクセスする場合であってもID番号およびパスワードを何度も繰返し入力する必要のない企業内通信システムおよび認証サーバを提供することを目的とする。

【0004】

【課題を解決するための手段】 上記課題を解決するため、請求項1の発明にかかる企業内通信システムでは、サーバコンピュータと複数のユーザ端末からなり、前記サーバコンピュータが様々なサービスを提供する企業内通信システムにおいて、前記サーバコンピュータは、前記サービスへのアクセス権限を標章する複数の鍵を保持する鍵データベースと、ユーザ毎に登録される識別情報とパスワードとを含むユーザ情報データベースと、ユーザに対して割当てられた鍵とユーザ名とを対にして保持する認証テーブルと、前記ユーザ情報データベースを参照してユーザの正当性を判定するユーザ情報管理部と、該ユーザ情報管理部で正当なユーザであると判定されたときにユーザ端末に対して前記鍵を割当てる認証処理部とを有し、前記ユーザ端末は、前記サーバコンピュータによって割当てられた鍵を受信し、前記サーバコンピュータの提供するサービスにアクセスする際に、アクセス要求に前記割当てられた鍵を含めることを特徴とする。このような構成により、一度の認証手続のみで繰返しサービスの提供を受けることが可能となる。また請求項3

にかかる発明では、請求項1記載の企業内通信システムにおいて、前記サーバコンピュータによって前記ユーザ端末に割当てられた鍵は、一定時間が経過すると無効することを特徴とする。

【0005】このような構成により、ユーザと鍵との対応関係が定期的に変更されるため、不正なアクセスを防止し、システムの安全性が向上する。さらに請求項4の発明にかかる認証サーバでは、サービスを提供するサーバコンピュータへアクセスするため、ユーザ端末からの認証要求に基づき認証処理を実行する認証サーバにおいて、前記サービスへのアクセス権限を標章する複数の鍵を保持する鍵データベースと、ユーザ毎に登録される識別情報とパスワードとを含むユーザ情報データベースと、ユーザに対して割当てられた鍵とユーザ名とを対にして保持する認証テーブルと、前記ユーザ情報データベースを参照してユーザの正当性を判定するユーザ情報管理部と、該ユーザ情報管理部で正当なユーザであると判定されたときにユーザ端末に対して前記鍵を割当てる認証処理部とを具備したことを特徴とする。このような構成により、ユーザが煩雑な認証処理を経ることなくサービスの提供を受けることが可能となる。

【0006】

【発明の実施の形態】以下、添付の図面を参照して本発明の実施の形態について説明する。図1は、本発明の企業内通信システムの構成を示す図であり、2台のサーバコンピュータ1、2とユーザ端末3からなり、またサーバコンピュータ1、2及びユーザ端末3はネットワーク4によって接続されている。また、サーバコンピュータ1は、ネットワーク4を介してパケットの送受信を行うインタフェース10、インタフェース10を介して受信したパケットの種別を判別し、ユーザからの各種要求を処理するアクセス処理部11、アクセス処理部11からのユーザ認証要求に基づいて、ID番号とパスワードが予め登録されているものであるか認証するとともに、後述の認証処理部にユーザの登録・鍵発行要求を行うID管理部12、ID管理部からの登録・鍵発行要求に応じて鍵の発行処理と鍵を与えたユーザと発行した鍵の対応関係を登録し、さらにアクセス処理部11からの認証要求に応じてアクセスを許可するための認証を行う認証処理部13、ユーザのID番号とパスワードが登録されID管理部12からアクセスされるIDテーブル14、認証処理部13によってアクセスされ、発行した鍵とユーザの情報を登録する認証テーブル15、多数の鍵を保持する鍵データベース（鍵DB）16、そしてユーザに対して各種サービスを提供するアプリケーション17とを有している。

【0007】なお、サーバコンピュータ1と2は同様の構成であるため、内部の構成はサーバコンピュータ1についてのみ説明し、サーバコンピュータ2ではその説明を省略する。また、上述の鍵とは文字または数字、もし

くは双方によって構成される。以下、上述の認証システムの動作について説明する。なお、ここでは、サーバコンピュータ1を人事情報閲覧用のサーバ、そしてサーバコンピュータ2を特許情報閲覧用のサーバとして説明する。まず、ユーザ（ユーザ名を「ユーザ1」とする。）がユーザ端末3を使用してサーバコンピュータ1の人事情報へのアクセスを行う場合、ブラウザソフトウェアなどを起動させてメニュー画面を表示させる。このときの画面は、例えば図2に示すように人事情報にアクセスするためのメニュー21、特許情報にアクセスするためのメニュー22等が表示される。ここでユーザは、ユーザ端末3に備えられているポインティングデバイス（図示せず）を操作してメニュー21を選択する。メニュー21が選択されると、ユーザ端末3からはサーバコンピュータ1を宛先とするアクセス要求が出力され、ネットワーク4を介してサーバコンピュータ1に受信される。

【0008】受信されたアクセス要求は、インタフェース10を介してアクセス処理部11に渡される。アクセス処理部11では、受信したアクセス要求の判定を行うが、ここでの判定は前記アクセス要求に鍵が含まれているか否かについてなされる。もし、パケットに鍵が含まれていない場合には、初回のアクセスであると判断し、ID番号とパスワードを入力させるための画面情報をユーザ端末3に対して送信する。この画面情報を受信したユーザ端末3のディスプレイ上には、図3に示すようにID番号とパスワードを入力するための画面31が展開される。ユーザは、この画面31に対して自己のID番号とパスワードの入力を行うが、ここで、入力されるユーザのパスワードは「PASSWORD1」、そしてID番号を「1111111」とする。入力されたパスワードとID番号は、ネットワーク4およびサーバコンピュータ1のインタフェース10を介して再びアクセス処理部11によって受信され、ID管理部12に対してパスワードとID番号の認証要求がなされる。ID管理部12が前記認証要求を受けると、ユーザによって入力されたIDとパスワードとID番号がIDテーブル12に登録されているかの確認を行う。

【0009】図4は、IDテーブル14に登録されているパスワードとID番号の状態を示したもので、ID管理部12は、IDテーブル14と比較を行い正当なユーザであるかの認証を行う。ここでは、ユーザによって入力されたパスワードが「PASSWORD1」で、かつID番号が「1111111」であり、IDテーブル14に登録されているため、ID管理部12は正当なユーザであると判断し、認証処理部13に対してユーザ名と、鍵の発行要求を出力する。認証処理部13は、ID管理部12からの鍵発行要求を受けると、鍵DB16を検索し、未発行の鍵を選択してアクセス要求を行ったユーザに対して発行処理を行い、認証テーブル15の更新処理を実行する。認証テーブル15は、例えば図5に示

すように「鍵番号」、「ユーザ名」とを含んでおり、鍵の発行により発行した鍵の鍵番号（ここでは「鍵1」を発行したとする。）とユーザ名に「ユーザ1」が登録される。発行された鍵1は、ネットワーク4を介してユーザ端末3によって受信され、以後、サーバコンピュータ1およびサーバコンピュータ2へアクセスする際には、アクセス要求にかかるパケットには発行された鍵1が含まれる。

【0010】ユーザ端末3のユーザは、前にも述べたように、人事情報の閲覧を実行しようとしているため、鍵1の発行が完了すると、この鍵1を含んだパケットを用いて再びサーバコンピュータ1のアクセスを実行する。サーバコンピュータ1のアクセス処理部11は、前記人事情報に対するアクセス要求にかかるパケットを受信すると、前述と同様に鍵が含まれているかのチェックを実行する。ここでは、発行された鍵1が含まれているため、鍵が含まれていると判定されて、認証処理部13に対して、鍵の正当性の判断を要求する。認証処理部13では、正当性の判断要求を受け付けると、パケットに含まれている鍵とユーザ名が認証テーブル15に登録されているかのチェックを行うが、認証テーブル15には鍵1とユーザ1が対になって登録されているため、アクセス処理部11に対してアクセスを許可する旨の通知がなされる。もし、アプリケーション17に対するアクセス要求にかかるパケットに鍵が含まれている場合であっても、鍵とユーザ名とが対になった情報が認証テーブル15に登録されていない場合には、認証処理部13からアクセス処理部11へはアクセスを許可しない旨の通知がなされる。

【0011】また、このように登録されていない鍵とユーザ名に基づいたアクセスがあった場合には、不正なアクセスと看做してシステム管理者へ通知するようにしてもよい。なお、一度発行された鍵はその後のアクセスに繰り返し利用可能であり、また、鍵の発行がサーバコンピュータ1によってなされた場合であっても、サーバコンピュータ2へのアクセスにも利用することが可能である。ただし、鍵を発行したサーバコンピュータ1ではないサーバコンピュータ2へアクセスする場合には、両サーバコンピュータの認証テーブルを同期させる必要があるため、サーバコンピュータ1の認証テーブル15が更新されると、直後または定期的に、この更新された情報を他のサーバコンピュータ2へ通知し同期を図る必要がある。また、セキュリティの面から一度発行した鍵がある一定時間経過した場合には無効にするような仕組みを取り入れることも可能である。この場合は、認証テーブル15は図6に示すように、「ユーザ名」、「鍵番号」そして「時間」からなり、この時間は鍵発行時に有効時間が設定され、以後カウントダウンされてゼロになったときに鍵を無効とする。また、前記時間は、鍵発行時の時刻に有効時間を加えたものとし、この時刻に達したと

きに鍵を無効としてもよいし、有効期限は鍵を発行した日が終わるまでとしてもよい。

【0012】さらに、ユーザの意志に基づき鍵を返却（無効化）する機能を附してもよい。この場合は、メニュー画面上に鍵返却ボタンを設け、ユーザがこの鍵返却ボタンを選択することによって、アクセス処理部11を介して認証処理部13に鍵の無効化要求が伝わり、認証テーブル15中の該当するユーザ登録が抹消されることになる。また、ユーザに対して割当てる鍵に権限の強弱をつけることも可能である。即ち、ユーザの役職などの立場によってアクセス可能なサービスに制限を課すことである。この場合、IDテーブル14に登録される情報は、「ユーザ名」、「ID番号」、「パスワード」の他に、全てのサービスにアクセス可能な特権を持ったユーザであることを示す「特権情報」が付加され、また鍵DB16には、通常の鍵以外に特権鍵が存在することになる。以上述べたように、企業内通信システムで提供される様々なサービスにアクセスする場合であっても、ユーザにとっては煩雑な認証手続きを繰り返す必要がなくなる。また、発行した鍵に有効期限を附した場合には、鍵が割当てられたユーザと、鍵との対が定期的に変更になるため、登録された情報の不正使用を防止することが可能となる。

【0013】さらに、鍵毎にアクセス可能なサービスを制限することによって、本来アクセスすべきユーザにのみアクセスを制限することが可能となる。続いて、本発明の他の実施の形態について説明する。図7は、他の実施の形態に係る企業内通信システムの構成を示した図であり、図1に示したシステムと異なる点は、鍵を割当てる専用のサーバコンピュータ（以下、認証サーバと称する。）71が、各種のサービスを提供するサーバコンピュータ72と独立して存在することであり、他には同様の構成要素であるネットワーク4とユーザ端末710が存在する。さらに、認証サーバ71は、ネットワーク4とパケットの送受信を行うためのインタフェース711、ユーザ端末710の利用者であるユーザの正当性を確認するとともに鍵の割り当て要求を行うID管理部712、ID管理部712からの鍵割り当て要求を受けて鍵の割り当てを行うとともに、サーバコンピュータ72に対して鍵を割当てたユーザに関する情報を送信する鍵発行部713、ユーザのID番号とパスワードが登録されているIDテーブル714、そして複数の鍵が登録されている鍵データベース716とを有しており、一方サーバコンピュータ72は、ネットワーク4とパケットの送受信を行うためのインタフェース717、ユーザ端末710からのアクセス要求を処理するアクセス処理部718、前記アクセス要求に含まれる鍵によってアクセスを許可するか否かを認証する認証処理部719、ユーザに対して各種のサービスを提供するアプリケーション720、そして割当てられた鍵とユーザの情報を登録する

認証テーブル721とを有している。

【0014】以下、上記システムの動作について説明する。まず、ユーザはユーザ端末710を操作してサーバコンピュータ71に対して鍵の発行要求を行う。この発行要求はインタフェース711を介してID管理部712によって受信される。ID管理部712は、前記発行要求を受けると、ユーザ端末3に対してID番号とパスワードの入力を促す画面を送信する。ユーザ端末710からID番号とパスワードが送信されると、ID管理部712は、IDテーブル714を参照して正当なユーザであるかの確認を行い、正当なユーザ、即ち入力されたID番号とパスワードがIDテーブル714に登録されていた場合には鍵発行部713に対して鍵の割当て要求を行う。この要求を受けると、鍵発行部713は、鍵DB716を検索して未割当ての鍵をユーザ端末710に送信するとともに、サーバコンピュータ72の認証テーブル721に発行した鍵とユーザ名からなる情報を登録させる。ユーザ端末710は、サーバコンピュータ71から鍵の割当てを受けてサーバコンピュータ72からサービスの提供を受けることが可能となり、アプリケーション720に対してアクセス要求を送信する。

【0015】このアクセス要求は、インタフェース717を介して認証処理部719によって受信され、認証テーブル721に登録されている鍵とユーザ名であるか認証が行われる。この認証によって、認証テーブル721に登録されているユーザ名と鍵を含んでいることが確認できると、認証処理部719はアクセス処理部718に対してアプリケーション720へのアクセスを許可する旨の通知を行い、アクセス処理部717は前記通知を受けてユーザ端末710に対して要求されたサービスの提供を行う。このようにして割当てられた鍵は、上述のように、自主的な返却或使用期限が到来するまで繰り返し使用することが可能であるため、煩雑な認証手続きをアクセスの度に行うことなくサービスの提供を受けることが可能となる。また、この例では鍵を管理するサーバコンピュータが1台のみであるため、安全性も向上させることが可能である。なお、ここでは鍵を発行する専用の

サーバコンピュータを含むシステムとして説明したが、鍵を発行する機器はルータやゲートウェイのネットワーク接続装置であっても構わない。

【0016】

【発明の効果】以上説明したように、本発明によると、ユーザが企業内通信システム（イントラネット）で提供されている様々なサービスにアクセスする場合であっても、一度の認証、即ちアクセス権を表す鍵の発行を受けると、以後のアクセス時には認証が不要となるため、煩雑な手続きを経ることなくサービスの提供を受けることが可能となる。

【図面の簡単な説明】

【図1】 本発明の実施の形態にかかる企業内通信システムの構成を示す図。

【図2】 ユーザ端末に表示されるメニュー画面の一例を示す図。

【図3】 ユーザ端末に表示されるID情報とパスワードの入力画面の一例を示す図。

【図4】 IDテーブルの一例を示す図。

【図5】 認証テーブルの一例を示す図。

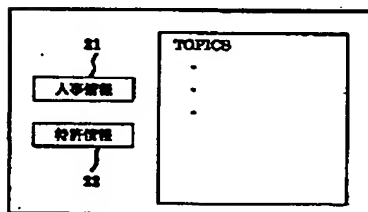
【図6】 認証テーブルの他の例を示す図。

【図7】 本発明の他の実施の形態にかかる企業内通信システムの構成を示す図。

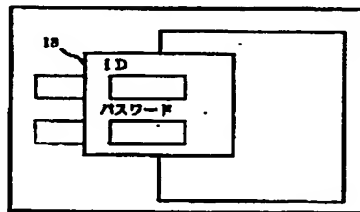
【符号の説明】

- 1, 2, 71, 72…サーバコンピュータ
- 3, 710…ユーザ端末
- 4…ネットワーク
- 10, 711, 717…インタフェース
- 11, 718…アクセス処理部
- 12, 712…ID管理部
- 13, 719…認証処理部
- 14, 714…IDテーブル
- 15, 721…認証テーブル
- 16, 715…鍵データベース
- 17, 720…アプリケーション
- 21, 22…アクセス要求ボタン
- 31…ID情報とパスワードの入力画面

【図2】



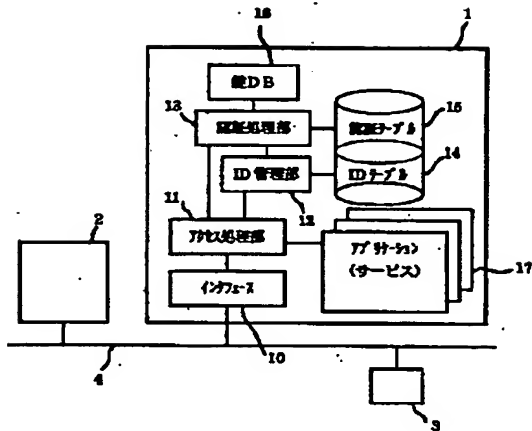
【図3】



【図5】

鍵番号	ユーザ名
鍵1	ユーザ1

【図1】



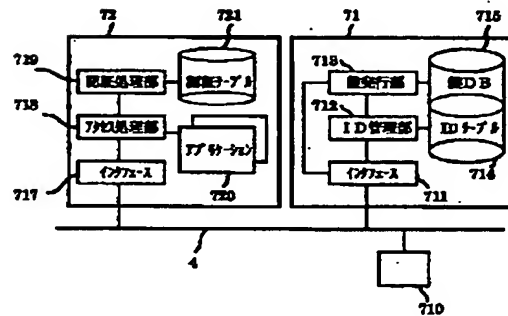
【図4】

ユーザ名	ID番号	パスワード
ユーザ1	1111111	PASSWORD1
ユーザ2	2222222	PASSWORD2

【図6】

機番	ユーザ名	時間(分)
機1	ユーザ1	120

【図7】



フロントページの続き

Fターム(参考) 5B085 AE00 AE02 AE03
 5J104 AA07 AA16 EA01 EA16 KA01
 KA02 MA06 NA02 NA05 NA36
 NA38 PA07